Coventry City Council

Briefing note

To: Audit and Procurement Committee **Date: 19 February 2018**

Subject: Information Commissioner's Office – Data Protection Audit November 2017

1 Purpose of the Note

1.1 In October 2015, the Information Commissioner's Office (ICO) carried out a data protection audit into the City Council's governance arrangements, training and awareness and data sharing arrangements. The audit concluded that there was "very limited assurance that processes and procedures are in place and deliver data protection compliance." The Audit and Procurement Committee has received regular reports on progress since that Initial audit. In November 2017, the ICO carried out a re-audit and this note reports on the findings and the Council's response.

2 Recommendations

Audit and Procurement Committee is recommended to:

a) Note the outcome of the ICO audit
b) Note the actions taken and planned in response to the audit
c) Request feedback on progress against actions arising from the audit
d) Make any recommendations to the Cabinet Member for Policy and Leadership who is the portfolio holder for information management and governance

3 Information/Background

3.1 In October 2015, the Information Commissioner's Office (ICO) carried out a data protection audit into the City Council's governance arrangements, training and awareness and data sharing arrangements. In addition to meeting with officers responsible for corporate arrangements, it spoke to staff in Children's Social Care and the Revenues and Benefits service.

3.2 The audit concluded that there was "very limited assurance that processes and procedures are in place and deliver data protection compliance." It made 77 recommendations for the Council to strengthen its arrangements which the City Council has implemented as part of a significant programme of work to strengthen its approach to information governance. The Audit and Procurement Committee has received regular reports on progress against the ICO's recommendations since then.

3.3 In November 2017 the ICO revisited the authority to carry out a further data protection audit. It followed exactly the same scope, looking at governance arrangements, training and awareness and data sharing arrangements corporately and in Children's Social Care and the Revenues and Benefits service. As previously, the audit provides a snapshot of assurance levels at a moment in time rather than specifically looking at the direction of travel or progress since the previous audit.

3.4 The outcome of the November 2017 audit is that the ICO has raised their overall opinion level to “limited assurance”. This reflects progress in both the overall rating and the three areas reviewed by the ICO and this is shown in the tables below.

2015 Audit

	Overall	DP Governance	Training and Awareness	Data Sharing
High				
Reasonable				
Limited				
Very Limited				

2017 Audit

	Overall	DP Governance	Training and Awareness	Data Sharing
High				
Reasonable				
Limited				
Very Limited				

3.5 In commenting on the progress made by the City Council, the ICO’s Lead Auditor, who was a member of the ICO team for both audits wrote that “*in our view, comparison between the assurance ratings strongly reflects on the work undertaken at CCC since our original audit. … This demonstrates a clear improvement and progress at an individual, as well as an overall, level”.*

3.6 The ICO report makes 141 detailed recommendations for the Council to consider, some of which are duplicated.

- 18 recommendations have been rejected as arrangements are already in place to address the issues raised;
- 32 have already been completed as they proposed only very minor amendments to processes or documents;
- 91 fall into three main areas where the Council has further work to do. Many of them support existing planned action, particularly work being undertaken to ensure the City Council is ready for the introduction of the General Data Protection Regulation in May 2018. These are:

3.6.1 **Information Risk Management:** Since the previous audit, the City Council has developed its approach to information risk management and put in place policies, procedures and oversight to ensure that risks to information are managed effectively. Information governance is highlighted on the corporate risk register, appropriate roles and responsibilities have been designated and risk management has improved. However, work is still required to populate and review information risk registers and this is currently being rolled out. When this is embedded, this will significantly strengthen the Council’s management of information risk.

3.6.2 **Training:** The ICO audit recognises the considerable work that has gone into strengthening data protection training and awareness raising across the Council and this is reflected in the reasonable assurance rating given to this area. This includes the work undertaken by the Information Management Strategy Group to ensure that appropriate training, including the mandatory training for all staff, is carried out which is highlighted as good practice. However, the audit report recommends the introduction of a comprehensive training strategy to address the Council's approach to general and specialist training. This is accepted and is in preparation.

3.6.3 **Data Sharing:** The Council's data sharing arrangements have improved significantly since the time of the initial audit and this part of the report includes the fewest number of recommendations. The recommendations that are made focus on improving the consistency and robustness of arrangements and these are accepted. The Council's Information Governance Team will continue to work with services to strengthen this area of work.

3.7 The City Council has developed its own action plan in response to the recommendations by the ICO and this is set out at Appendix 1. The Executive Summary of the ICO audit report is included at Appendix 2.

Adrian West
Members and Elections Team Manager
adrian.west@coventry.gov.uk
024 7683 2286

Appendix 1

Data Protection Governance

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
1	A9, A11	Review Job descriptions in the Information Governance Team as part of the planned restructure following recent staff and organisational changes. We have in the meantime clearly allocated line management responsibility.	May-18	Members and Elections Team Manager
2	A26a, A28a, A90, A91, A94	Make available templates for policies, procedures and guidance ensuring document control is included. Create a policy index to signpost to the single version of each policy as prescribed by the Information Governance handbook and incorporate date of review to ensure clarity and regular review.	Apr-18	Records Manager
3	A27, A34a, A36	Fully implement the Information Risk Management Process, including the completion of the Information Risk Registers by Information Asset Owners, regular review of the Information Asset Regsiter and the process for providing formal assurance to the Senior Information Risk Owner on relevant information assets. The duties responsibilities for risk escalation are already detailed within the Council's Risk Management Policy, Strategy and Framework. The Information Asset Register and Information Risk Register will then be subject to annual review.	Jul-18	Head of Information Governance
4	A28b	Update the risk management framework to cross-reference to the Information Risk Policy and Registers. The Risk Management Policy and Strategy will be updated during the next review cycle.	Mar-18	Head of Information Governance
5	A31	The Senior Information Risk Owner is to nominate an alternative Officer to act as Information Asset Owner for his services	Jul-18	Senior Information Risk Owner
6	A37	Implement and raise awareness of a formal and documented Information Security Incident Management Policy (building on the existing draft procedures), which outlines objectives, key roles and responsibilities, a process flowchart and detailed guidance as to the various stages of the incident management process	Mar-18	Head of Information Governance
7	A52, A68	Consider the best method of linking the Corporate Risk Register and the Information Risk Register/Information Asset Register to ensure that information risks can be escalated appropriately and consistently as required.	Jul-18	Head of Information Governance / Insurance Manager
8	A54, A55a, A55b, A56, A58	Ensure that the contract template and live contracts consistently incorporate the requirement for data processors to act only on their instruction. This will be completed as part of our preparations for GDPR	May-18	Head of Information Governance

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
9	A59, A63	Draft, implement and raise awareness of a formal and documented Privacy Impact Assessment Policy, which outlines objectives, key roles and responsibilities, a process flowchart and detailed guidance as to the various stages of the PIA process. Ensure that this policy is cross-referenced within other associated data protection policies.	May-18	Head of Information Governance
10	A66	Ensure that the Privacy Impact Assessment register includes hyperlinks to copies of the individual Privacy Impact Assessments where possible.	Aug-18	Head of Information Governance
11	A74	Consider aligning the Council to external standards to improve the effectiveness of data handling controls, for example by consistently benchmarking data protection policies against these.	May-18	Information Management Strategy Group
12	A76	Establish a comprehensive range of formal documented data protection Key Performance Indicators, report against these on an ongoing basis and ensure that the audience for this reporting includes the Corporate Leadership Team and Information Management Strategy Group, in order to facilitate a high level view of organisational performance.	Jun-18	Information Management Strategy Group
13	A81, A82, A87, A88, A92, A93, A100	Undertake an annual review of all Information Governance Policies within the Information Governance Handbook, and ensure consistent branding. This will need to also consider changes for May 2018 and the introduction of GDPR.	May-18	Records Manager
14	A83	Amend the Information Security Management Policy to outline the responsibilities of individuals and teams and / or groups with core information security roles, and provide an overview of key aspects of information security such as incident management and physical security. Amend the Data Handling Policy to provide content in regard to corporate data handling requirements.	Apr-18	Head of Information Governance
15	A96, A106	Consider the best method of ensuring that communications are received, read and understood by using GovDelivery or similar tools to provide data and evidence of users accessing material that is shared.	Dec-18	Head of Communications

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
16	A99	Develop a more in depth series of checks in respect of the main themes of data protection compliance such as information security and records management, either within the same or dedicated checklists, and periodically rotate between conducting such checks. For example, checks in regard to information security could include physical access to and within Council buildings, access to manual records storage in open office areas, adherence to clear desk and screen, and the disposal of electronic hardware and manual records.	Aug-18	Head of Information Governance

Training and Awareness

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
1	A7, A61, A78, B2, B10, B14, B18, B22, B30, B35, B40, B41, B42, B43, B50, B53, B72	Compile a training strategy to formally document the approach taken to training. The strategy will contain: - Training objectives - Training methods - Available courses and the mix of mandatory, specialist and non-mandatory training. - Alternative training methods for non-networked, agency and 3rd party staff - How training will be evaluated - How take up is monitored - Roles and responsibilities in ensuring compliance	31st March 2018	Programme Manager (Transformation)
2	B2, B4, B5, B74, B78	Update the Information Governance Handbook, and suite of Data Protection policies to include the roles and responsibilities of the Senior Information Risk Owner, Data Protection Officer and Information Management Strategy Group in relation to training	31st March 2018	Programme Manager (Transformation)
3	B21	Utilise functionality in the recently implemented online learning system (Me-Learning), to enable feedback to be provided by trainees on course material and to use that feedback to inform future training provision.	31st March 2018	Programme Manager (Transformation)
4	B26	Include further detail on Subject Access Requests and Cyber-Security into the mandatory training.	31st March 2018	Programme Manager (Transformation)
5	A103, A104, B32, B36	Ensure that induction checklists consistently document the requirement for mandatory training to be completed, with links to the policies and training. This is to be extended to all staff including temporary and agency staff.	31st March 2018	Programme Manager (Transformation)

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
6	B34	Ensure that agency staff have clear instructions on how to access the newly implemented online learning platform (Me-Learning)	31st March 2018	Programme Manager (Transformation)
7	B54	Finalise a communications plan which covers the requirements for training to be completed, together with periodic communications covering Data Protection awareness themes.	31st March 2018	Programme Manager (Transformation)

Data Sharing

Action No	ICO ref. no	Agreed Action	Implementation Date	Owner
1	c2, a26a, a92	Create and enforce use of a Policy Template, ensure it states that policies are subject to annual review and contains the appropriate document control.	May-18	Records Manager
2	c8	Enforce the process that requires staff that are involved in one-off data sharing undertake the relevant training	Mar-18	Information Governance Team/Senior Management
3	c10	Consider merging the Privacy Policy and the Corporate Privacy Statement, make available form the website homepage and that it provides links to the Current Data Sharing agreements	May-18	Information Governance Team/Information Management Strategy Group
4	c12	Implement a formal sign-off process for and register of, Privacy Notices, to ensure corporate oversight fo the fair processing information provided	Jun-18	Senior Information Governance Officer
5	c14, c21	Review the Data Sharing training and incorporate new requirements under GDPR. Create and provide guidance for staff around use of the Data Sharing protocol rather than a Data Sharing Agreement.	May-18	Senior Information Governance Officer

6	c19	Carry out a review of the Privacy Impact Assessment template; ensure template specifies which Data Protection Act condition for processing or exemption applies.	Jun-18	Senior Information Governance Officer/ Information Governance Team
7	c22, c30, c31, c32, c33, c34, c37, c13	Ensure that all Data Sharing Agreements: - Include statements of compliance signed by senior management of each participating Data Controller. - Consistently detail whether information to be shared is fact or opinion. - Consistently outline a requirement for the sender of the information to inform recipients when data has been amended or updated. - Implement processes to ensure the information received and being shared as part of a DSA is accurate and up to date. - Amend DSA template to facilitate compliance to the fifth principle of the Data Protection Act. - Contain consistent requirements for the secure disposal of information in line with Retention & Disposal Schedule. - Include a requirement for 3rd parties to notify the Council when information is deleted. - Include a clause stating how a Data Breach should be reported and a specific timeframe given. - Consistently provide details of how fair processing information will be given to individuals	May-18	Senior Information Governance Officer/ Information Governance Team
8	c23	Approve the MASH Partnership Agreement as soon as possible.	Feb-18	Senior Information Governance Officer
9	c26	Review all Council contract templates in preparation for GDPR to ensure their compliance with the Regulation. Undertake a review of existing contracts.	May-18	Information Governance Officer/Contracts Manager
10	c42	Ensure that the Information Management Strategy Group have access to central log for one-off disclosures.	May-18	Information Governance Team/ Information Management Strategy Group